UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,165	10/31/2003	Jonathan D. Herbach	07844-623001	1607

21876   7590   08/26/2010
FISH & RICHARDSON P.C.
P.O. Box 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER
DUNN, DARRIN D

ART UNIT	PAPER NUMBER
2121	

NOTIFICATION DATE	DELIVERY MODE
08/26/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

<table>
<tr><td rowspan="3">Office Action Summary</td><td>Application No.
10/699,165</td><td>Applicant(s)
HERBACH ET AL.</td><td></td></tr>
<tr><td>Examiner
DARRIN DUNN</td><td>Art Unit
2121</td><td></td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>03 August 2010</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-8, 23-29 and 35-41</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-8, 23-29, and 35-41</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   The Office Action is responsive to the communication filed on 08/03/2010.

2.   Claims 1-8, 23-29, and 35-41 are pending in the application.

Provisional Support

Object Identifiers, Download Request to Server from Client

60/490810 – content identifiers supported in ([06] e.g., list of known objects for download). [07]

–user selects objects for download, [10] – description for each object)

Download Manager Program

60/500388 – [05] – motivation for integrating software functionality together (e.g., functions

depicted in Doyle for user authentication based on action types and selected files may be

integrated as part of the download manager, as discussed below)

60/508626 – [03], [08] e.g., motivation to expand upon rights enforced via the download

manager based on existing functions of controlling rights to a file which supports motivation to

integrate the functions of a) user authentication and b) use restrictions within the download

manager upon a user selecting a file for download)

Response to Amendment

3.   Applicant's request for reconsideration of the finality of the rejection of the last Office

action is persuasive and, therefore, the finality of that action is withdrawn.

Response to Arguments

4.   Applicant's arguments with respect to claims 1,3, and 23 have been considered but are

moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.   The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness under 35

U.S.C. 103(a) are summarized as follows:

    1.   Determining the scope and contents of the prior art.
    2.   Ascertaining the differences between the prior art and the claims at issue.
    3.   Resolving the level of ordinary skill in the pertinent art.
    4.   Considering objective evidence present in the application indicating obviousness or nonobviousness.

7.   Claims 1, 3-4, 6, 23, 28, 36-37, and 39 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Doyle et al. (USPN 7515717) in view over Raciborski et al. (PGPub

20050132083) and in further view over Heath et al. (USPN 6006034)

8.   As per claim 1, Doyle et al. teaches a method comprising:

    receiving, at a server, a request from a client to take an action with respect to an electronic

document ([Col 1 lines 36-46] e.g., furthermore, as discussed below, the download manager, as

per Raciborski et al., clients, running a download manager, request files from a media server for

download);

retrieving a document identifier (e.g., as interpreted, the type of document) from the request

([Col 1 lines 61-67], [Col 2 lines 18-20, lines 43-48, lines 65-67], [Col 20 lines 62-67] e.g., text

file, or per-document, image, or a particular file (document, message, etc). Moreover, as per

Reciborski et al., teaches the use of content descriptions [0032- object descriptions, involved for

indentifying content for download) ;

determining whether user authentication is needed based on the document identifier (e.g. as

interpreted, the type of document) and the action (e.g., access) ([Col 9 lines 16-20, lines 43-48] ,

[Col 1 lines 36-46], [Col 8 lines 38-49] e.g., authentication of the user based upon a file request,

where a file request corresponds to multiple types of files, where a file type is identified as being

at least one of a text, message, or a per-document request). * The Examiner notes the Doyle et

al. teaches the pertinent functions of requesting a file from a server, associating use restrictions

for the file based on granularity of the file, authentication a user for the file, and controlling an

action ([Col 1 lines 36-46]) These functions are executed via software ([Col 24 lines 5-20]) that

may be combined with a download manager, as discussed below.

A] **Software Program for use in identifying a current user and controlling an action with
respect to the document based on the current user and document permissions**

However, Doyle et al. does not teach sending information specifying an acceptable

authentication procedure. First, please note that the following discussion will modify the

download manager to incorporate the functions of authenticating a user and restricting access to downloading a file based on an action. Second, the "information" shall be addressed in part B].

Raciborski et al. teaches a download manager, i.e., program invoking an authentication but is silent as to the program invoking a) user authentication and b) file restrictions based on the user and action type. Doyle et al. teaches the software functions of a) authenticating a user, determining the type of action the user is permitted to perform on the file but is silent as to doing this for a specific file type (e.g., document identifier) ([Col 1 lines 36-46]) Raciborski et al. teaches identifying the file for download based on a content identifier ([0032], [0025] e.g., description for each object). Raciborski et al. further teaches an action pertaining to a file (e.g., downloading the file)

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to modify the download manager to include the functions of authenticating a user accessing a file, identifying a file type that is being accessed, and implementing restrictions for the user attempting to access the file (e.g., action). **60/500388 – [05]** teaches that software functions may be integrated. In effect, as modified, a download manager functions as a software program enabling download of a file and requiring authentication of the who user who requests the file (e.g., content identifiers- as modified, file types correspond to audio, video, or per-document) to determine whether to provide the file (e.g., action), and what operations the user is allowed to perform on it (e.g., actions)

B] Sending information specifying an acceptable authentication procedure (e.g., a program, i.e., download manager, that effectuates user authentication using a password procedure ([Col 9 lines 16-25])

Heath et al. teaches a server running multiple versions of application software residing on a

server where the server functions to provide programs, files, and data for client computers ([Col

1 lines 6-26]).   Heath et al. further teaches providing 'information" to a client regarding a

program but not with regard to the program characterized as an authentication procedure ([Col 1

lines 60-67] e.g., catalog)

Therefore, at the time the invention was made, one of ordinary skill in the art would have

motivation to first store multiple versions of a download manager on a server, as per Heath et al.,

whereby the server functions as a media server, as per Raciborski et al. comprising a download

manager for download to a client computer. As per Heath et al., it is obvious that a server may

provide a program to the client, which in this case is a download manager. Based on file requests

from a client running a version of the download manager, as per Rociborski et al., this may

represent a call, as per Heath et al. ([Col 1 lines 63-65], to the server. In effect, it is obvious this

"call" represents an opportunity to check for updates (e.g., subsequent to the client requesting a

file for download). The server, in response, sends "information specifying an acceptable

authentication procedure" (e.g., version of the download manager to the client running a version

of the download manager)

As modified, Heath et al. teaches receiving an authentication procedure update request (e.g.,

as interpreted, requesting a new version of the download manager ([Col 1 lines 56-67], [Col 2

lines 1-10] e.g., the download manager comprises an authentication procedure, i.e, three part

authentication) from the client in response to client processing of the information specifying an

acceptable authentication procedure (e.g., catalog pertaining to version of the download manager

embodying password procedures, as per Doyle et al. ([Col 9 lines 16-24]);

obtaining, at the server and in response to the authentication procedure update request, a software program (e.g., new version of the download manager) comprising instructions operable to cause one or more data processing apparatus to perform operations effectuating the authentication procedure (e.g. as per Doyle et al., Col 9 lines 16-24]); and

sending the software program to the client for use in identifying a current user and controlling the action with respect to the electronic document based on the current user and document-permissions information ([Col 8 lines 38-45], [Col 1 lines 36-46] e.g., permission to download, permission to read, write, permission to copy. The pertinent functions are embodied in the download manager, based on motivation to integrate software functions in a central program) associated with the electronic document (e.g. as per Heath et al., [Col 2 lines 1-5] e.g., an new version of the download manager is downloaded to the client as part of the version updating process, [Col 1 lines 38-40]. Supra Doyle et al. ([Col 1 lines 36-46])

5.   Claims 2, 24 ,and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (USPN 7515717) in view over Raciborski et al. (PGPub 20050132083) in view over Heath et al. (USPN 6006034) and in further view over Kano et al. (USPN 20030135650)

6.   As per claims 2, 24, and 35, Raciborski et al. does not teach a second server providing the software program. Kano et al. teaches a backup server ([ABSTRACT])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to include a backup server as a means of providing redundancy. In the event of a failure of the primary server, it would have been beneficial to utilize a backup server as a means of distributing the software program, modules, and versions as they become available.

9.   As per claim 3, Doyle et al., as modified ,teaches

receiving, at a server, a request from a client to take an action with respect to an electronic

document ([Col 1 lines 36-46] e.g., as modified, a client, running a version of the download

manager, sends a request to a media server to download a file. As modified, the download

manager verifies the user, determines the document type, and whether to permit a download to

occur)

obtaining, at the server and in response to the request, a software program (e.g., download

manager version) comprising instructions operable to cause one or more data processing

apparatus to perform operations effecting an authentication procedure (e.g., supra claim 1, Doyle

et al., [Col 9 lines 16-24]);

sending the software program to the client for use in identifying a current user and controlling

the action with respect to the electronic document based on the current user and

document-permissions information associated with the electronic document (e.g., supra claim 1);

receiving an updated authentication procedure (e.g., supra claim 1, i.e., new version of the

download manager);

receiving a subsequent request from the client to take the action with respect to the electronic

document (e.g., it is implied from Rociborski et al. that users make additional download request

using the download manager for a file resident on a media server. It is obvious that subsequent

requests will be invoked to enable users to obtain media files. The subsequent request entails an

action (e.g., download);

obtaining, at the server and in response to the subsequent request, a new software program

comprising instructions operable to cause one or more data processing apparatus to perform

operations effecting the updated authentication procedure (e.g., supra claim 1 discussion, where a

new version of the download manager is obtained where a new version entails an updated

software set of the authentication procedure, as per Col 9 lines 16-24] e.g., although the whole

program is updated, which in effect encompasses the authentication portion, it's obvious that any

portion of the software may be updated, as per Heath et al., [Col 1 lines 50-55]. As applied, it is

obvious that any portion of a program can be updated, including the authentication portion of the

download manager)

; and

    sending the new software program to the client for use in identifying the current user and

controlling the action with respect to the electronic document based on the current user and the

document-permissions information associated with the electronic document (e.g., supra claim 1)

10.   As per claims 4 and 37, Raciborski et al. teaches software program uses an existing

interface provided by the client to communicate authentication information to the server ([FIG

2A-208])

11.   Claims 5, 26, and 38 are rejected under 35 U.S.C. 103 as being unpatentable over Doyle

et al. (USPN 7515717) in view over Raciborski et al. (PGPub 20050132083) in view over Heath

et al. (USPN 6006034) and in further view over view over Hu (USPN 5586260)

12.   As per claims 5, 26, and 38, Raciborski et al., as modified by Doyle teaches receiving

credentials information from the client derived at least in part based on input obtained by the

client using the software program (e.g., download manager using authentication, [Col 9 lines 16-

25]) but does not teach communicating with a third part authentication server to authenticate the

current user based on the credentials information. Hu teaches a third party authentication server

([ABSTRACT])

Therefore, at the time the invention was made, one of ordinary skill in the art would have motivation to implement a third party authentication server as taught by Hu et al. Hu teaches a method for authenticating a client for a server. Raciborski teaches a system for authenticating a user/client to enable access to content stored on a server. Since a third party authentication server provides a well known means in which to maintain, store, and retrieve credentials, it would have been advantageous to provide this server as an additional means, in effect providing both redundancy in addition to reducing load on the primary server.

13.   As per claims 6 and 39 Doyle et al. teaches the method of claim 5, wherein the input obtained by the client comprises text input ([Col 9 lines 26-35]).

14.   Claims 7 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al. (USPN 7515717) in view over Raciborski et al. (PGPub 20050132083) in view over Heath et al. (USPN 6006034) in view over Hu (USPN 5586260) and in further view over Leon (PGPub 20040249765)

15.   As per claims 7 and 40, Doyle et al. teaches the method of claim 5 but does not teach wherein the input obtained by the client comprises biometric data ([0043] e.g., biometric authentication). Leon teaches biometric authentication ([ABSTRACT])

Therefore, at the time the invention was made ,one of ordinary skill in the art would have motivation to modify Doyle et al. to include biometric information as part of the authentication procedure. Doyle et al. teaches a three step authentication means involving passwords. Leon teaches the use of biometric information in user authentication. Therefore, it would have been obvious to implement biometric authentication as a further means to ascertain someone's identify.

16.   As per claims 8,27, 38, and 41, Raciborski et al., as modified by Doyle et al., teaches

receiving input from a client using the software (e.g., download manager using password

authentication, Col 9 lines 16-26). It does not teach receiving an authentication receipt from a

third party authentication server based on input obtained by the client using the software. Hu

teaches returning an access key from an authentication gateway acting as a proxy server to the

client, i.e., receipt, based on credentials ([ABSTRACT], [COL 1 lines 58-63] e.g., receiving an

authentication receipt from a third party authentication server) and verifying the current user

with the third party authentication server using the authentication receipt ([COL 1 lines 18-20],

lines 59-63], [ABSTRACT] e.g., authenticating a client)

    Therefore, at the time the invention was made, it would have been obvious to have provided a

means in which to authenticate a client via saving security credentials,. Doyle et al. teaches

authenticating a user via credentials as to enable access to content on a server. Hu et al. teaches

saving security credentials for later use and generating an access key for their retrieval and

passing the access key to the client. In effect, saving the security credentials for later use and

providing an access key for their retrieval obviates the need for repeated authentication. As a

result, the system is further optimized and limits redundant authentication procedures.

17.   As per claim 23, Doyle et al., as modified, teaches a system comprising:

    a client that sends an authentication procedure update request to a server in

response to client processing of information received from the server (supra claim 1), wherein

the information received from the server specifies one or more acceptable authentication

procedures (e.g. versions of the download manager, supra claim 1);

the server that receives the authentication procedure update request, and in response to the client,

the server obtains and sends a software program comprising instructions operable to cause one or

more data processing apparatus to perform operations effecting an authentication procedure

(supra claim 1); and

wherein the client uses the software program to identify the current user and control an action

with respect to an electronic document based on the current user and document- permissions

information associated with the electronic document, and wherein the action comprises an action

taken with respect to the electronic document subsequent to opening the electronic document at

the client (e.g., supra claim 1)

18.   Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Doyle et al.

(USPN 7515717) in view over Raciborski et al. (PGPub 20050132083) and in further view over

Heath et al. (USPN 6006034) and in further view over Boozer et al. (USPN 7370344)

19.   As per claim 25, Raciborski et al., as modified, teaches the system of claim 23 but does

not teach wherein the client includes a security handler. Raciborski et al, teaches a server-

communication interface (e.g., web browser) to the software program (e.g., download manager)

([Figure 2B]. Boozer et al. teaches a security handler (64) for receiving a request and examining

whether the request should be granted ([Col 2 lines 20-29])

   Therefore, at the time the invention was made, one of ordinary skill in the art would have

motivation to modify Raciborski et al., in view over Doyle et al., to integrate a security handler,

as per Boozer et al., to verify whether a request to access content within the media server should

be granted. The motivation is to cope with a diverse set of users and ensure that only trusted

users may gain initial access to the information. The security handler provides an additional

layer of protection on top of the download manager's authentication procedure.

19.   As per claim 28, Raciborski et al., as modified, teaches a server comprising:

a server core with configuration and logging components ([0029])

an internal services component that provides functionality across dynamically loaded

methods ([0029] e.g., web page)

dynamically loaded external services providers, including an authentication service

provide (supra Hu for authentication server - ABSTRACT)

20.   Claim 29 is rejected under rejected under 35 U.S.C. 103(a) as being unpatentable over

Doyle et al. (USPN 7515717) in view over Raciborski et al. (PGPub 20050132083) in view over

Heath et al. (USPN 6006034) in view over Hu (USPN 5586260) and in further view over

Tenerelllo (USPN 7233981)

7.   As per claim 29, Raciborski et al. teaches a business logic tier comprising a cluster of

document control servers ([0029] e.g. content delivery networks); an application tier including

the client comprising a viewer client, a securing client, and an administration client ([FIG 1-FIG

2A – client computer functions via providing a view – browser, securing – downloading the

manager (securing a program), and administration (storage media)). However, Racoborski et al.

does not teach a load balancer that routes client requests to the document control server.

Tenerello teaches a system and method for load balancing ([COL 1 lines 14-20], [COL 2 lines

63-67])

Therefore, at the time the invention was made, one of ordinary skill would have motivation

to load balance a system. Raciborski et al. teaches that various user computers may access

content objects ([0029]) Tenerello teaches a load balancing means in which multiple requests

may be efficiently processed. Since load balancing increases performance of a system, it would

have been obvious to have enabled a system employing multiple user computers, each requesting

access to a resource, a means to load balance the requests as to optimize the system.

21.   As per claim 36, Doyle et al., as modified, teaches the system of claim 23, wherein the

server receives a subsequent request from the client to take the action with respect to the

electronic document (e.g., supra claim 23), obtains, in response to the subsequent request, a new

authentication process, and sends the new authentication process to the client for use in

identifying the current user and controlling the action with respect to the electronic document

based on the current user and the document- permissions information associated with the

electronic document (e.g. supra claim 23)

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to DARRIN DUNN whose telephone number is (571)270-1645.

The examiner can normally be reached on EST:M-R(8:00-5:00) 9/5/4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Albert DeCady can be reached on (571) 272-3819. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DD/   /Albert DeCady/
08/20/10   Supervisory Patent Examiner
                                                Art Unit 2121